EXHIBIT 13

Remediate denied access with the Policy Remediator

Preview — Policy Remediator

This feature is subject to the "Pre-GA Offerings Terms" in the General Service Terms section of the Service Specific Terms (/terms/service-terms#1). Pre-GA features are available "as is" and might have limited support. For more information, see the launch stage descriptions (/products#product-launch-stages).

This page shows you how to enable and use the Chrome Enterprise Premium Policy Remediator.

Save page

When users attempt to access a Google Cloud resource but aren't compliant with the access policy for the resource, they are denied access and receive a general 403 error message. You can use the Policy Remediator to provide users with actionable steps that they can take to remediate their issue before reaching out to an admin for additional help. The specific remediation actions depend on the access policies, but can include things such as enabling screen lock, updating the operating system (OS) version, or accessing an app from a network allowed by your company.

Enable Policy Remediator

1. Grant your organization admin the `roles/policyremediatormanager.policyRemediatorAdmin` role at the organization level by running the following commands in the Google Cloud CLI:

```
gcloud organizations add-iam-policy-binding 'organizations/ORGANIZATION_ID
    --member PRINCIPAL \
    --role roles/policyremediatormanager.policyRemediatorAdmin
```

   Replace the following:

   - *ORGANIZATION_ID*: the Google Cloud organization ID.

Ex. 13

- ***PRINCIPAL***: the identifier for the principal, or member, which usually has the following form: `PRINCIPAL_TYPE:ID`. For example, `user:my-user@example.com`.

2. Enable the Policy Remediator Manager API by running the following command:

```
gcloud services enable policyremediatormanager.googleapis.com
```

3. Call the Policy Remediator Manager to enable Policy Remediator for the projects in an organization, this creates a service agent (/iam/docs/service-agents).

Save page

```
curl -X POST \
"https://policyremediatormanager.googleapis.com/v1alpha/organizations/ORGAN
--header 'Authorization: Bearer ACCESS_TOKEN' \
--header 'X-Goog-User-Project:PROJECT_ID'
```

Replace the following:

- ***ORGANIZATION_ID***: the Google Cloud organization ID.
- ***ACCESS_TOKEN***: use the following command to generate the access token.

```
gcloud auth print-access-token
```

- ***PROJECT_ID***: the Google Cloud project ID.

Following is an example response, which contains the service agent details:

```
{
"name": "organizations/ORGANIZATION_ID/locations/global/operations/",
"metadata": {
  "@type":
"type.googleapis.com/google.cloud.policyremediatormanager.remediatorservicei
a.OperationMetadata",
   "createTime": "",
```

Ex. 13

```
    "target": "organizations/ORGANIZATION_ID/locations/global/remediatorSe
    "verb": "update",
    "requestedCancellation": false,
    "apiVersion": "v1alpha"
  },
  "done": false
}
```

Where ***ORGANIZATION_ID*** is the Google Cloud organization ID.

4. In the Google Cloud CLI, run the following command to access the service agent that you created:

Save page

```
curl -X GET \
"https://policyremediatormanager.googleapis.com/v1alpha/organizations/ORGAN
--header 'Authorization: Bearer ACCESS_TOKEN' \
--header 'X-Goog-User-Project:PROJECT_ID'
```

Replace the following:

- ***ORGANIZATION_ID***: the Google Cloud organization ID.
- ***ACCESS_TOKEN***: use the following command to generate the access token.

```
gcloud auth print-access-token
```

- ***PROJECT_ID***: the Google Cloud project ID.

You should receive the service agent email in the following format:

```
{
"name": "organizations/ORGANIZATION_ID/locations/global/remediatorService
"state": "ENABLED",
```

Ex. 13

```
"serviceAccountEmail": "service-org-ORGANIZATION_ID@gcp-sa-v1-remediator.
}
```

Where ***ORGANIZATION_ID*** is the Google Cloud organization ID.

Assign the service agent role in the Google Admin console

1. Log in to the Google Admin console.

   Go to the Google Admin console (https://admin.google.com/ac/devices/list)

2. Go to **Account > Admin roles**, and then click **Create new role**.

   Save page

   - Enter a name and a description (optional) for the role, and then click **Continue**.
   - In **Admin console privileges**, go to **Services > Mobile and Device Management** and select the **Manages Devices and Settings** permission.
   - In **Admin API privileges**, go to **Groups**, and then select the **Read** permission.
   - Click **Continue**, confirm your entries, and complete creating the role.
   - Go to **Assign Service Accounts** and enter the email address of the newly created service agent (#service-acct-email).
   - Click **Add > Assign Role**.

3. In the Google Cloud CLI, run the following commands to grant the Service Agent (`policyremediator.serviceAgent`) role to the service agent at the organization level. This gives the service agent permission to read the Identity and Access Management and other access policies for your organization.

```
gcloud organizations add-iam-policy-binding 'organizations/' \
   --member='serviceAccount:service-org-ORGANIZATION_ID@gcp-sa-v1-remedia
   --role='roles/policyremediator.serviceAgent'
```

Replace ***ORGANIZATION_ID*** with the Google Cloud organization ID.

Ex. 13

Enable Policy Remediator for an IAP resource

You must have a Chrome Enterprise Premium license to use this feature.

1. Go to the Identity-Aware Proxy (IAP) page.

   Go to IAP (https://console.cloud.google.com/security/iap)

2. Select a resource, and then click **Settings**.

3. Go to **Remediate access**, and then select **Generate remediation actions**.

Grant the remediator role

Save page

To give users permission to remediate denied access to IAP resources, run the following command in the Google Cloud CLI:

```
gcloud iap web add-iam-policy-binding \
    --member='PRINCIPAL' \
    --role='roles/iap.remediatorUser'
```

Replace ***PRINCIPAL*** with an identifier for the principal, or member, which usually has the following form: `PRINCIPAL_TYPE:ID`. For example, `user:my-user@example.com`.

For additional information, see gcloud iap web add-iam-policy-binding (/sdk/gcloud/reference/iap/web/add-iam-policy-binding).

To give users permission to remediate access to IAP resources at a project level, run the following command in the Google Cloud CLI:

```
gcloud projects add-iam-policy-binding PROJECT_ID \
    --member PRINCIPAL \
    --role roles/iap.remediatorUser
```

Replace the following:

Ex. 13

- ***PROJECT_ID***: the Google Cloud project ID.
- ***PRINCIPAL***: the identifier for the principal, or member, which usually has the following form: `PRINCIPAL_TYPE:ID`. For example, `user:my-user@example.com`.

Remediate with the Help Desk

When end users are denied access, they are redirected to a Chrome Enterprise Premium page that contains troubleshooting information, including a troubleshooting URL and a remediation token. If users don't have permission to open the remediation token, they can copy the remediation token and send it to the Help Desk for additional help.

Save page

Policy attributes and associated messages

The following table provides the list of attributes that are supported by the Policy Remediator.

Attribute	Default message
`ip_address`	You`re accessing the app from a network not allowed by your company.
`region_code`	Access this app from a region allowed by your company.
`is_secured_with_screenlock`	Set a screen password on your device. Turn off the screen password on your device.
`verified_chrome_os`	Use a device with verified [OS type]. Use a device without verified [OS type].
`is_admin_approved_device`	Use a device approved by your organization administrator. Use a device not approved by your organization administrator.
`is_corp_owned_device`	Use a device owned by your organization. Use a device not owned by your organization.
`encryption_status`	Use an encrypted device. Use an unencrypted device.

Ex. 13

Attribute	Default message
`os_type`	Switch to a [OS type] device. [OS type] devices cannot access this app.
`os_version`	Update to an OS version that is at least [version]. Downgrade your OS to a version less than [version].

Troubleshooting

The Policy Remediator cannot generate remediations when any of the following occur:

- A resource has conflicting policies, such as a user must connect using Windows and macOS.

Save page

- The attribute is not supported by the Policy Remediator.
- The service agent does not have permission to remediate.

Last updated 2025-01-30 UTC.

Ex. 13